In The Specification:

Please amend the paragraph at page 1, lines 4-11 as indicated below:

The present invention is related to the following commonly-assigned U.S. patents, all of which were filed concurrently herewith: U.S. _____ (Ser. No. ~~09/_____~~) 09/761,906), entitled "Secure Integrated Device with Secure, Dynamically-Selectable Capabilities"; U.S. _____ (Ser. No. ~~09/_____~~) 09/764,844), entitled "Smart Card with Integrated Biometric Sensor"; U.S. _____ (Ser. No. ~~09/_____~~) 09/764,827, entitled "Technique for Continuous User Authentication"; U.S. _____ (Ser. No. ~~09/_____~~) 09/761,899), entitled "Technique for Establishing Provable Chain of Evidence"; and U.S. _____ (Ser. No. ~~09/_____~~) 09/765,127), entitled "Technique for Improved Audio Compression".

Please amend the paragraph at page 8 line 10 to page 9, line 2 as indicated below.

U.S. ~~Patent _____~~, Patent No. 6,772,331, entitled "Method and Apparatus for Exclusively Pairing Wireless Devices", (Ser. No. 09/316,686, filed May 21, 1999) taught a technique for establishing secure trusted relationships between devices in a Bluetooth network using special-purpose hardware, along with software on each device. The special-purpose hardware comprises, for example, a protected memory for storing a digital signature, where this memory is physically attached to the radio transmitter of each device; a display screen on at least one device capable of showing a media access control (MAC) address of the device; and an input button or other comparable device on at least one device for the user to indicate his assent to a trust relationship. While the disclosed technique provides security improvements for networking a collection of devices, there is a significant cost involved. Even if such an investment were made, the overall business process would remain unsecure against certain types of attacks. Furthermore, the disclosed technique cannot be applied to prior art smart credit cards, which have neither a display nor a button for indicating trust.

Please amend the paragraph at page 23, line 18 to page 24, line 21 as indicated below.

FIG. 2 depicts logic that may be used to implement preferred embodiments of the component authentication process of the present invention. This logic is executed when an application processor is plugged in to the application bus (Block 200). The act of plugging in the

processor causes a hardware reset (Block 210) of the application processor (at the electrical level). This hardware reset is preferably initiated as in the prior art, and clears the application processor's memory, sets all hardware components (such as I/O ports, interrupt controllers, timers, and direct memory access controllers) to a known initial state, and causes the application processor's CPU to start executing a predetermined instruction stream at a particular memory location. (This particular memory location is preferably an address within the application processor's ROM, or other on-board memory or storage.) The hardware reset is necessary so that the application processor will be in a known state, so that the security core can vouch for its state thereafter (for the interval over which the application processor remains continuously plugged in to the application bus). Among the initial instructions executed, according to the present invention, will be those required to perform a security handshake (Block 220) between the security core and the application processor. This security handshake is preferably an SSL-like handshake, and its purpose is mutual authentication between the two connecting devices. In preferred embodiments of the present invention, the security handshake is performed using the teachings of commonly-assigned U.S. ~~Patent~~ Patent No. 6,826,690 (Ser. No. 09/435,417), which is entitled "Using Device Certificates for Automated Authentication of Communicating Devices" and which is hereby incorporated herein by reference. According to these teachings, each device must be provided with a digital certificate and a private cryptographic key, as well as a unique device identifier (such as a MAC address or perhaps a serial number). For purposes of the present invention, the device identifier may be used later to uniquely and verifiably identify data streams coming from this application processor.